(ii) If authorized in Component instructions, wallet-size cards which describe in general terms the purpose(s) for authorizing the employee to remove classified material from the facility (for example, use at meetings or transmission to authorized recipients).

(3) Inspectors are to ensure that personnel are not removing classified material without authorization. Where inspectors determine that individuals do not appear to have appropriate authorization to remove classified material, they shall request such individual to obtain appropriate authorization before exiting the premises. If, due to the circumstances, this is not feasible, the inspector should attempt to verify by telephone the authority of the individual in question to remove the classified material with the employing office. When such verification cannot be obtained, and if removal cannot be prevented, the inspector shall advise the employing office and appropriate security office as soon as feasible that classified material was removed by the named individual at a particular time and without apparent authorization.

(4) If the employing office determines that classified material was removed by one of its employees without authority, it shall request an investigation of the circumstances of the removal by appropriate investigative authorities. Where such investigation confirms a violation of security procedures, other than espionage or deliberate compromise, for which §159a.50 applies, appropriate administrative, disciplinary, or legal action shall be taken.

Subpart G—Compromise of Classified Information

§159a.41 Policy.

Compromise of classified information presents a threat to the national security. Once a compromise is known to have occurred, the seriousness of damage to U.S. interests must be determined and appropriate measures taken to negate or minimize the adverse effect of such compromise. When possible, action also should be taken to regain custody of the documents or material that were compromised. In all cases, however, appropriate action must be taken to identify the source and reason for the compromise and remedial action taken to ensure further compromises do not occur. The provisions of DoD Instruction 5240.4[23] and DoD Directive 5210.50[24] apply to compromises covered by this subpart.

§159a.42 Cryptographic and sensitive compartmented information.

(a) The procedures for handling compromises of cryptographic information are set forth in NACSI 4006 and implementing instructions.

(b) The procedures for handling compromises of SCI information are set forth in DoD TS–5105.21–M–2[25] and DoD C–5105.21–M–1[26].

§159a.43 Responsibility of discoverer.

(a) Any person who has knowledge of the loss or possible compromise of classified information shall immediately report such fact to the security manager of the person's activity (see §159a.93(e)) or to the commanding officer or head of the activity in the security manager's absence.

(b) Any person who discovers classified information out of proper control shall take custody of such information and safeguard it in an appropriate manner, and shall notify immediately an appropriate security authority.

§159a.44 Preliminary inquiry.

The immediate commander, supervisor, security manager, or other authority shall initiate a preliminary inquiry to determine the circumstances surrounding the loss or possible compromise of classified information. The preliminary inquiry shall establish one of the following:

(a) That a loss or compromise of classified information did not occur;

(b) That a loss or compromise of classified information did occur but the compromise reasonably could not be expected to cause damage to the national security. If, in such instances, the official finds no indication of significant security weakness, the report

[23] See footnote 1 to §159a.3.
[24] See footnote 1 to §159a.3.
[25] See footnote 13 to §159a.33(j).
[26] See footnote 13 to §159a.33(j).